



Agency for Healthcare Research and Quality
Advancing Excellence in Health Care

North Carolina State University

On Learning about Certification through the Analysis of Open Source and Proprietary EHR Systems

Laurie Williams
Associate Professor

June 4, 2010

Open Source EHR Applications

Source code is freely available and customizable

However, a service contract for installation and support is inevitable

Often more than one service provider backs an open source EHR Application

Open source software is generally designed to be interoperable due to lack of motivation for *proprietary vendor lock in*

Who is motivated to pay for CCHIT certification?

Certification

To receive ARRA incentive and to avoid penalties, health care providers must utilize certified EHR systems

Currently, CCHIT is at the helm of EHR certification and the basis of our evaluation

Our focus to date

Functional certification test scripts

Does the application provide the functionality necessary to enable *meaningful use*?

Security certification test scripts (new in Oct 2009, for 2011)

Does the system protect patient data?

The Bad Guys: Who Wants to Do What with Patient Data? Just a sampling ...

Doctors

Malpractice suit? Erase the evidence!

Receptionists

Wondering if her neighbor has AIDS?

Insurance companies

Looking for pre-existing conditions?

Patients

Need to renew a prescription or erase a diagnosis?

Terrorists

Cause a system-wide denial of service

Disgruntled system administrators

Delete some data on the way out the door

Our Evaluation Journey

OpenMRS – Open Source

OpenEHR – Open Source

“ProprietaryMed” – Proprietary

Looking for generalized information about certification and **not incriminating these products!**

OpenMRS



Passed less than half of CCHIT functional test scripts

Design Flaws:

- Admin is super power

- No logging

- New users given customizable roles

- Users can “shop around” without a trace

... analysis abandoned (late 2009) because we felt it could not be used in the US without major revision; target customer base Africa

	OpenEMR	ProprietaryMed
License	GPL	Proprietary
Popularity	1168 downloads/mo	21,000 patient records
Size (SLOC/Files)	305,000 / 1,600	120,000 / 900
Version	3.2 (2/16/2010)	1.0 (3/31/2010)
Contributing Developers	18	12
Platform	PHP	ASP.NET
CCHIT Certified	In Process	In Process



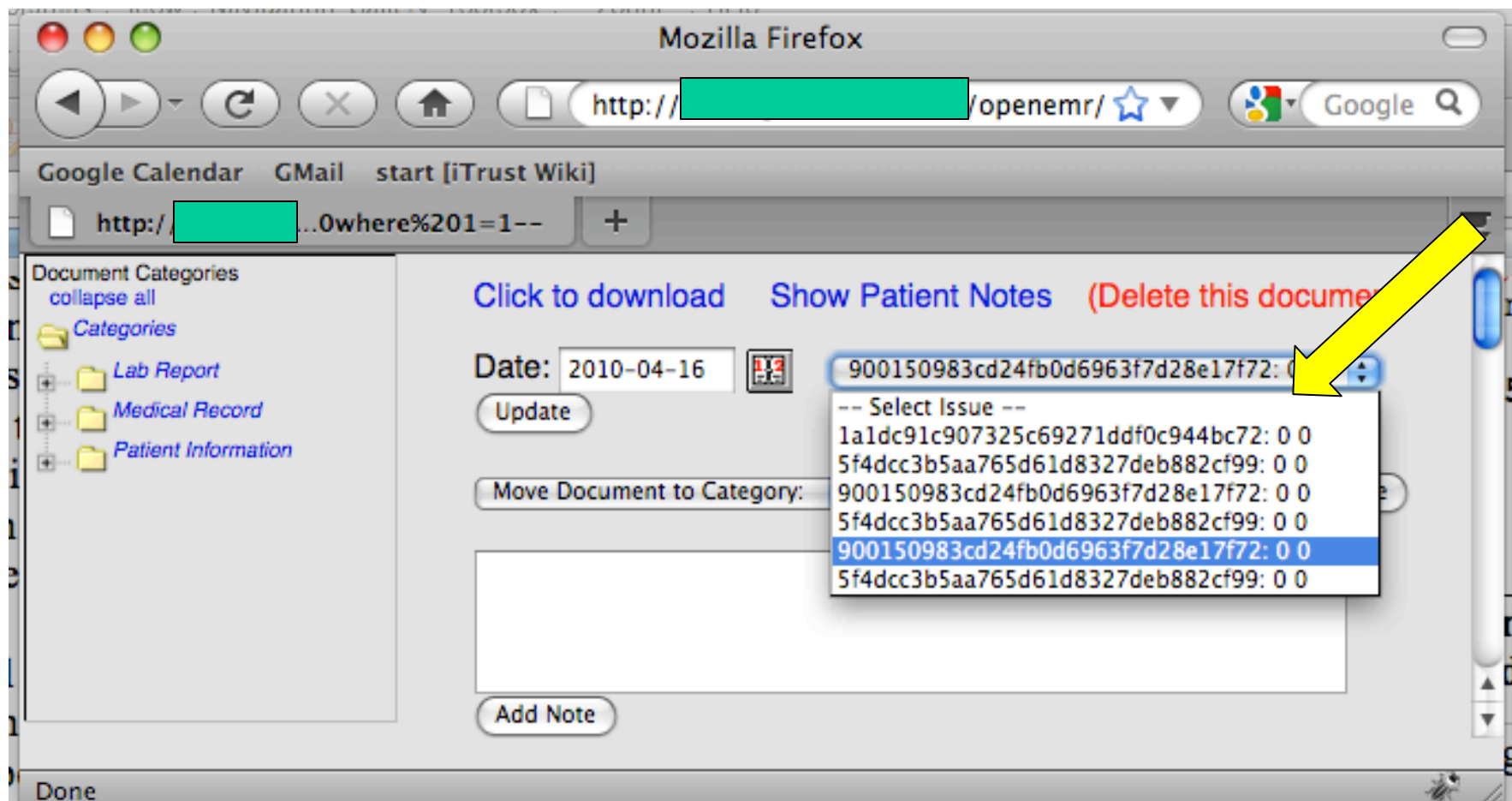
openEMR

Evaluation

“Red team” exploited vulnerabilities... selected successful attacks to follow ...

These would not be surfaced as issues by CCHIT security test scripts

OpenEMR: Obtain every user's username and password (SQL injection)



Both EHRs: Denial of Service (Cross-site Scripting)

Default

☒ Top
☒ Bot

Calendar

Patient/Client

Management

Visits

New Visit

Current

List

Transact

Chart Tracker

Visit Forms

Medical Record

Fees

Administration

Reports

Miscellaneous

Active Patient:

None

Active Encounter:

None

Popups


Find:

by: Name ID SSN DOB Any Filter

User Manual

Online Support

Logout



Reported Attack Page!

This web page at www.goooooogleadsence.biz has been reported as an attack page and has been blocked based on your security preferences.

Attack pages try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack pages intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here!

Why was this page blocked?

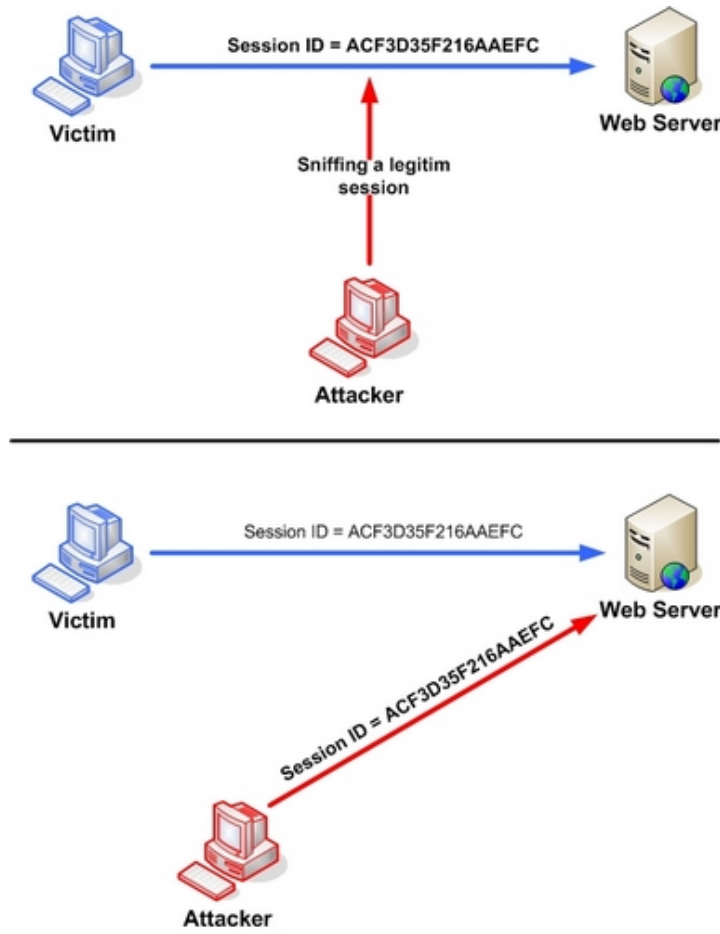
Ignore this warning

Patient Notes (See All) and Authorizations (More)

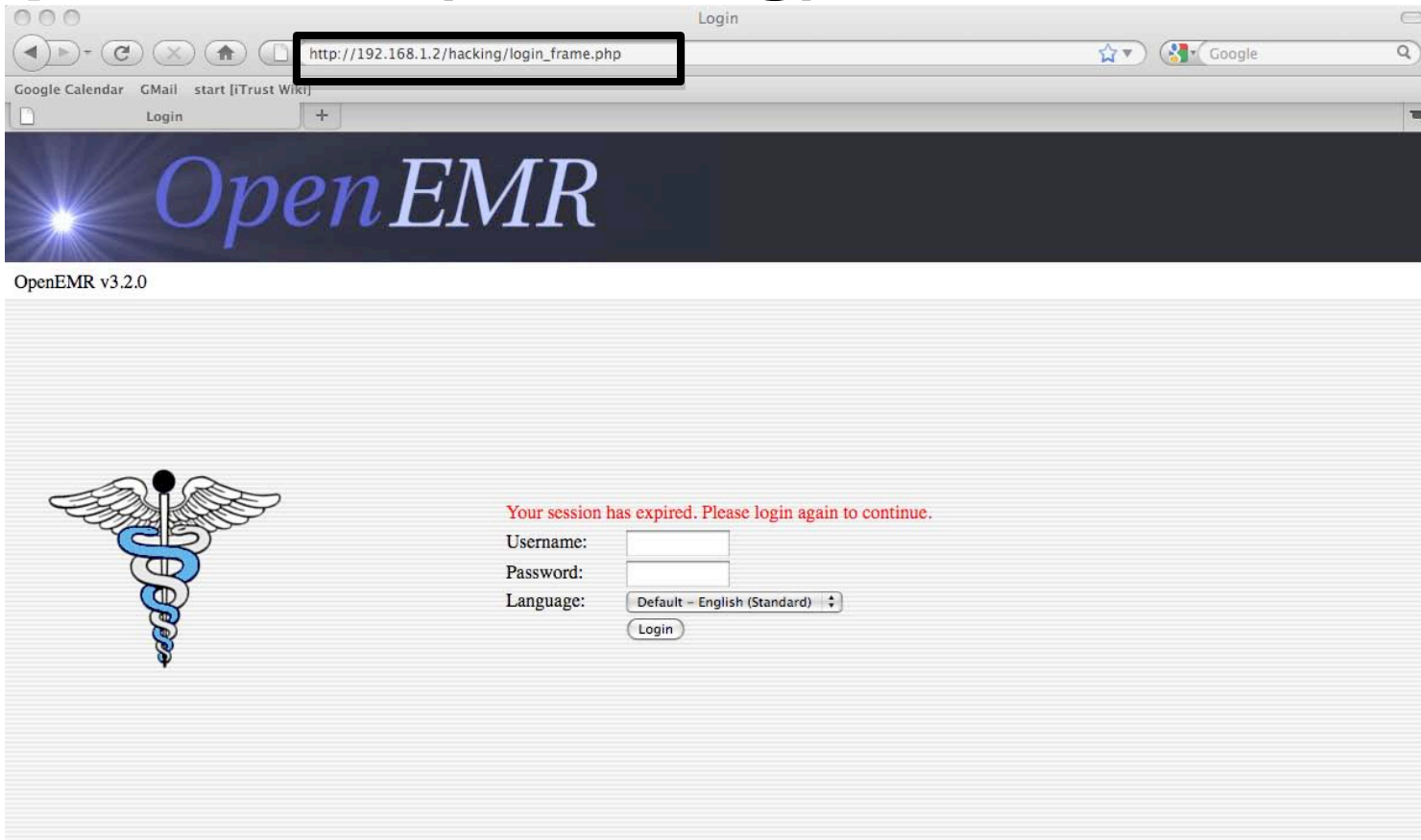
Patient	Note Type	Timestamp and Text
K, Jason	Unassigned	2010-04-12 18:36 (admin to admin)
		2010-04-12 18:41 (admin to admin)

10

Both EHRs: Login as another user (Session Hijacking)



Both EHRs: Obtain username and password (Phishing)



OpenEMR v3.2.0

Your session has expired. Please login again to continue.

Username:

Password:

Language:

Other Design Flaws

In OpenEMR, the administrator can *read or change* another user's password.

In ProprietaryMed, there is no logging of any transaction.

In ProprietaryMed, there is no authorization control on patient records.

Certifying there are no security vulnerabilities?

Not possible

Recommendation:

Security test scripts as certification entry criteria.

Message: If you can't demonstrate basic operational security, don't waste our time checking your functionality.



Madman attempting to empty the ocean with a spoon.

Future Work

Finish the evaluation of current EHR applications

Evaluate more applications

- Open source and proprietary

Systematic, repeatable security evaluation procedure

Recommendations to certification bodies based upon our empirical evaluation/data

Provide EHR system testbed on our virtual computing platform

More information: <http://agile.csc.ncsu.edu/healthcare>